Title	2次体上定義された$\mathbf{Q}$-curveの形式群に関する本田の定理について (代数的整数論とその周辺)
Author(s)	西来路, 文朗
Citation	数理解析研究所講究録 (1999), 1097: 144-150
Issue Date	1999-04
URL	http://hdl.handle.net/2433/63012
Right	
Type	Departmental Bulletin Paper
Textversion	publisher

数理解析研究所講究録
1097巻 1999年 144-150

2次体上定義された Q-curve の形式群に関する本田の定理について

大阪大学理学研究科博士課程3年　西来路 文朗 (Fumio Sairaiji)

1 序文

代数体上定義された楕円曲線は, その全ての $\mathbf{Q}$- 共役な楕円曲線達が互いに同種の時, $\mathbf{Q}$-curve と呼ばれる. 特に, $\mathbf{Q}$ 上定義された楕円曲線は $\mathbf{Q}$-curve である. 本稿では, $\mathbf{Q}$ 上定義された楕円曲線の形式群に関する本田 [6],[7] の定理を, $\mathbf{Q}$-curve の場合に, 定義体に関して拡張することについて述べる.

$\mathbf{Q}$ 上定義された楕円曲線 E から独立に定義される2つの形式群 : E の極小モデルの形式群 $\hat{E}$, E の L- 関数 $L(E/\mathbf{Q},s)$ の形式群 $\hat{L}$, は共に $\mathbf{Z}$ 上定義され, かつ, $\mathbf{Z}$ 上強同型であることが, 本田により知られている. この証明には, (1) $\mathbf{Z}$ 上の形式群の分類に関する Hasse の原理, (2) 本田による p- 進整数環 $\mathbf{Z}_p$ 上の形式群の分類理論, (3) $\mathbf{Z}_p$ 上の形式群 $\hat{E}$ の強同型類の完全不変量が, $L(E/\mathbf{Q},s)$ の Dirichlet 係数で決まる事実, を用いる. (1), (2) については, 代数体の整数環上でほぼ成立することが知られているが, (3) は, E 上の ℓ- 進表現に付随する L- 関数を考えたのでは, 定義体が $\mathbf{Q}$ の場合を除いて, 成立しない. そのため, 代数体の場合に本田の定理を得るためには, (3) が問題である.

E を2次体上定義された $\mathbf{Q}$-curve とし, E の Weil restriction A が実数乗法を持つと仮定する. この場合, E 上の ℓ- 進表現に付随する L- 関数以外に, A 上の λ- 進表現に付随する L- 関数達が, E に付随する L- 関数として考えられる. 本稿では, この λ- 進表現に付随する L- 関数達の一次結合で得られるある L- 関数に対して, 技術的な仮定の下, 本田の定理を拡張する. 結果の応用として, 具体的に形式群 $\hat{E}$ を計算することにより, A の λ- 進表現に付随する L- 関数の Dirichlet 係数が求められる.

第2節で形式群に関する基本的な事柄を復習し, 第3節では, $\mathbf{Q}$ 上定義された楕円曲線の形式群に関する本田の定理を紹介する. 第4節では, 主結果, 計算例について述べる.

2 標数0の可換整域上の形式群

可換環 R 上の n 変数形式的べき級数環を, $R[[x_1,\cdots,x_n]]$ とおく. 特に1変数の場合には, $R[[x_1]]$ のかわりに, $R[[x]]$ とおく. $R[[x_1,\cdots,x_n]]$ の2元 φ,ψ の (total) degree $d-1$ 次以下の項が等しい時, $\varphi\equiv\psi \bmod \deg d$ と書く.

$$R[[x_1,\cdots,x_n]]_0 := \{\varphi\in R[[x_1,\cdots,x_n]] | \varphi\equiv 0 \bmod \deg 1\}$$

とおく. $\varphi(x)\in R[[x]]_0$ の1次の係数が R の単元である時, $\varphi(x)$ は invertible であると言う. この時, $R[[x]]_0$ の元 $\psi(x)$ で, $\varphi(\psi(x))=\psi(\varphi(x))=x$ をみたすものが唯一つ存在する. $\varphi^{-1}(x):=\psi(x)$ と書く.

Definition 2.1 $F(x_1,x_2)\in R[[x_1,x_2]]$ が次の条件 $(i)-(iii)$ をみたす時, $F(x_1,x_2)$ を R 上の (1変数可換) 形式群と呼ぶ.

$$\begin{aligned}(i)\quad & F(x_1,x_2)\equiv x_1+x_2 \ mod\ deg\ 2\\ (ii)\quad & F(F(x_1,x_2),x_3)=F(x_1,F(x_2,x_3))\\ (iii)\quad & F(x_1,x_2)=F(x_2,x_1)\end{aligned}$$

例えば, 加法群 $\hat{G}_a(x_1,x_2):=x_1+x_2$, 乗法群 $\hat{G}_m(x_1,x_2):=x_1+x_2+x_1x_2$ は, 共に, R 上の形式群である.

$F(x_1,x_2),G(x_1,x_2)$ を R 上の形式群とし, $\varphi(x)\in R[[x]]_0$ とする. $\varphi(x)$ が $F(x_1,x_2)$ から $G(x_1,x_2)$ への (R 上の) 準同型であるとは,

$$\varphi(F(x_1,x_2))=G(\varphi(x_1),\varphi(x_2))$$

をみたすことを言う. 準同型 $\varphi:F\to G$ が invertible である時, $\varphi^{-1}(x)$ は $G(x_1,x_2)$ から $F(x_1,x_2)$ への準同型となる. このような $\varphi(x)$ を弱同型と呼ぶ. さらに, 弱同型 $\varphi(x)$ が

$$\varphi(x)\equiv x \bmod \deg 2$$

をみたす時, $\varphi(x)$ を強同型と言う.

R 上の強同型 (resp. 弱同型): $F\to G$ が存在することを

$$F\approx_R G \quad (\text{resp. } F\sim_R G)$$

と書く. 関係 $\approx_R$ (resp. $\sim_R$) は同値関係である.

以下, R は標数 0 の可換整域, K を R の商体とする. R 上の形式群は自然に K 上の形式群となる.

Theorem 2.2 *(cf. [6])* R 上の形式群 $F(x_1,x_2)$ に対し, R の商体 K 上の強同型 $f:F\to\hat{G}_a$ が唯一つ存在する.

Theorem 2.2 における K 上の強同型 $f:F\to\hat{G}_a$ を $F(x_1,x_2)$ の変換子と呼ぶ.

$$f(F(x_1,x_2))=\hat{G}_a(f(x_1),f(x_2))=f(x_1)+f(x_2)$$

が成立することより, 形式群 $F(x_1,x_2)$ は

$$F(x_1,x_2)=f^{-1}(f(x_1)+f(x_2))$$

と書かれる.

形式群 $G(x_1,x_2)$ の変換子を $g(x)$ とおく. Theorem 2.2 により, $F(x_1,x_2)$, $G(x_1,x_2)$ は K 上では強同型で, 強同型 $F\to G$ は, $g^{-1}(f(x))$ で与えられる. それ故, $F\approx_R G$ は,

$g^{-1}(f(x)) \in R[[x]]$ と同値である. 特に, R が有限次代数体 k の極大整数環 $\mathcal{O}_k$ である場合, 次の意味で, Hasse の原理 :

$$F \approx_{\mathcal{O}_k} G \Longleftrightarrow \mathcal{O}_k \text{ の全ての素イデアル } \mathfrak{p} \text{ に対して, } F \approx_{\mathcal{O}_{k,\mathfrak{p}}} G$$

が成立する. 但し, $\mathcal{O}_{k,\mathfrak{p}}$ は $\mathcal{O}_k$ の $\mathfrak{p}$ に対する $\mathfrak{p}$- 進完備化である.

$\mathfrak{p}$- 進整数環 $\mathcal{O}_{k,\mathfrak{p}}$ 上の形式群の分類理論は, 本田 [7] により, $\mathfrak{p}$ が不分岐の場合には完全に, $\mathfrak{p}$ が分岐の場合にも殆ど, 完成されている.

楕円曲線の Weierstrass モデルに付随する形式群を定義する. R を標数 0 の可換整域, K をその商体とする.

E を R 係数の Weierstrass モデル

$$E : Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6 \quad (A_1, \cdots, A_6 \in R)$$

で定義された, 無限遠点を零点に持つ, K 上の楕円曲線とする. $T := -X/Y$ とおく時, T は E の零点における局所変数である. この局所変数 T に対して, E の不変微分 $w_E := dX/(2Y + A_1X + A_3)$ を展開し,

$$w_E = \sum_{n \geq 1} b_n T^n dT/T$$

とおく. $b_n \in R$, かつ, $b_1 = 1$ である. Weierstrass モデル E に付随する形式群 $\hat{E}(x_1, x_2)$ を

$$\hat{E}(x_1, x_2) := f_E^{-1}(f_E(x_1) + f_E(x_2)), \quad f_E(x) := \sum_{n \geq 1} \frac{b_n}{n} x^n$$

により定義する. この時, $\hat{E}(x_1, x_2) \in R[[x_1, x_2]]$ となることが知られている. 即ち, $\hat{E}(x_1, x_2)$ は R 上の形式群である (cf. [4],[10]).

以下の 3 , 4 節においては, Weierstrass モデル E に対し, 記号 $w_E, T, b_n, \hat{E}(x_1, x_2), f_E(x)$ を上の意味で用いる.

3 Q 上定義された楕円曲線の形式群

E を $\mathbf{Z}$ 係数の Weierstrass モデル

$$E : Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6 \quad (A_1, \cdots, A_6 \in \mathbf{Z})$$

で定義された $\mathbf{Q}$ 上の楕円曲線とする. 簡単の為, Weierstrass モデル E は極小モデルであると仮定する.

$L(E/\mathbf{Q}, s)$ を E 上の ℓ- 進表現に付随する L- 関数とする. $L(E/\mathbf{Q}, s)$ を Dirichlet 級数に展開し,

$$L(E/\mathbf{Q}, s) = \sum_{n \geq 1} \frac{a_n}{n^s}$$

とおく. $a_n \in \mathbf{Z}$, かつ, $a_1 = 1$ である. L- 関数 $L(E/\mathbf{Q}, s)$ に付随する形式群 $\hat{L}(x_1, x_2)$ を

$$\hat{L}(x_1, x_2) := g^{-1}(g(x_1) + g(x_2)), \quad g(x) := \sum_{n \geq 1} \frac{a_n}{n} x^n$$

により定義する.

Theorem 3.1 *(Honda [6],[7])* $\hat{L}(x_1, x_2)$ は $\boldsymbol{Z}$ 上の形式群であり, かつ, $\hat{L}(x_1, x_2)$ は $\hat{E}(x_1, x_2)$ と $\boldsymbol{Z}$ 上強同型である.

ここで, $\varphi(x) \in \mathbf{Z}[[x]]_0$ が, $\hat{L}(x_1, x_2)$ から $\hat{E}(x_1, x_2)$ への強同型であることは, $T = \varphi(S)$ とおいて局所変数 T を S に変数変換する時,

$$w_E = \sum_{n \geq 1} b_n T^n dT/T = \sum_{n \geq 1} a_n S^n dS/S$$

が成立することと同値である.

Theorem 3.1 は, $\hat{E}(x_1, x_2), \hat{L}(x_1, x_2)$ の変換子 $f_E(x), g(x)$ の係数 b_n, a_n $(n = 1, 2, \cdots)$ 達の間の合同式としても書ける. 特に次の系を得る.

Corollary 3.2 *(Honda [6],[7])* 任意の素数 p に対し, $a_p \equiv b_p \ mod\, p$ が成立する.

a_p の絶対値について, Weil の評価式 : $|a_p| \leq 2\sqrt{p}$ が知られている. $p \geq 17$ の時, $2\sqrt{p} < p/2$ であるから, Corollary 3.2 により, 少なくとも $p \geq 17$ においては, b_p の p を法としての絶対値最小の剰余が a_p である. また, Corollary 3.2 の合同式の代わりに, Theorem 3.1 から得られる別の p のべきを法とする合同式を用いれば, $p \leq 13$ においても, $b_p, b_{p^2}, b_{p^3}, \cdots$ 達から, a_p を決定することができる. このように, 具体的に $\hat{E}$ が与えられれば, b_n 達から, $L(E/\mathbf{Q}, s)$ の Dirichlet 係数が決定することができる.

4 2次体上定義された Q- 曲線の形式群

k を判別式 D_k の 2 次体, $\mathcal{O}_k$ を k の極大整数環とする. 2 次拡大 $k/\mathbf{Q}$ のガロワ群の生成元を σ で表す.

E を $\mathcal{O}_k$ 係数の Weierstrass モデル

$$E : Y^2 + A_1XY + A_3Y = X^3 + A_2X^2 + A_4X + A_6 \quad (A_1, \cdots, A_6 \in \mathcal{O}_k)$$

で定義された k 上の楕円曲線とする. 簡単の為, E が global minimal モデルを持つ場合のみを扱い, E は global minimal モデルであると仮定する. さらに, 次の条件 $(Ei) - (Eiv)$ を仮定する:

(Ei) k 上定義された次数 d の同種写像 $\varphi : E \to E^\sigma$ が存在する;

(Eii) d は square-free$\neq 1$;

$(Eiii)$ $\varphi^*(w_{E^\sigma}) = \alpha w_E$ をみたす $\mathcal{O}_k$ の元 α が存在する;

(Eiv) $\alpha\alpha^\sigma = d$.

条件 (Ei) により, E は $\mathbf{Q}$-curve である. また, 条件 $(Eii),(Eiii)$ は同種写像 $\varphi : E \to E^\sigma$ が形式群 $\hat{E}$ から $\hat{E}^\sigma$ への $\mathcal{O}_k$ 上の準同型を引き起こす為の十分条件である. これらの条件の下で, E に付随する L- 関数 $L_\alpha(s)$ を以下のように作る.

A を E の Weil restriction とする. A は $\mathbf{Q}$ 上定義された 2 次元アーベル多様体で, k 上では $E \times E^\sigma$ と同型になる. さらに, 条件 $(Ei),(Eii),(Eiv)$ より, $\varphi \times \varphi^\sigma : E \times E^\sigma \to E^\sigma \times E$ と自然な置換 : $E^\sigma \times E \to E \times E^\sigma$ との合成で得られる $E \times E^\sigma$ の自己準同型は A の $\sqrt{d}$-倍写像を引き起こす. この対応により, 埋めこみ写像

$$\iota : \mathbf{Q}(\sqrt{d}) \hookrightarrow \mathbf{Q} \otimes_Z \mathrm{End}_Q(A)$$

が得られる. 即ち, (A, ι) は $\mathbf{Q}$ 上 type $\mathbf{Q}(\sqrt{d})$ である.

$L(A, \iota, s)$ を (A, ι) 上の λ- 進表現の L- 関数とする. τ を 2 次拡大体 $\mathbf{Q}(\sqrt{d})/\mathbf{Q}$ のガロワ群の生成元とする時,

$$L(A, \iota, s)L(A, \iota \circ \tau, s) = L(A/\mathbf{Q}, s) = L(E/k, s)$$

が成立する. 但し, $L(A/\mathbf{Q}, s), L(E/k, s)$ は, それぞれ, A, E 上の ℓ- 進表現に付随する L- 関数である. (A, ι) は, type $\mathbf{Q}(\sqrt{d})$ だから, $L(A, \iota, s)$ は $\mathbf{Q}(\sqrt{d})$ 係数の Dirichlet 級数に展開される.

$$L(A, \iota, s) = \sum_{n \geq 1} \frac{c_n}{n^s}$$

とおく. 今の場合, $c_1 = 1$, かつ,

$$\begin{cases} c_n \in \mathbf{Z} & \text{if } (D_k/n) = 0, 1 \\ c_n \in \mathbf{Z}\sqrt{d} & \text{if } (D_k/n) = -1 \end{cases}$$

が成立する. 但し, (D_k/n) は Kronecker symbol を表す.

自然数 n に対し,

$$\tilde{c_n} = \begin{cases} c_n & \text{if } (D_k/n) = 0, 1 \\ (c_n/\sqrt{d})\alpha^\sigma & \text{if } (D_k/n) = -1 \end{cases}$$

により, $\tilde{c}_n$ を定める. 作り方から, $\tilde{c}_n \in \mathcal{O}_k$, かつ, $\tilde{c}_1 = 1$ である. Weierstrass モデル E に付随する L- 関数 $L_\alpha(s)$ を

$$L_\alpha(s) := \sum_{n \geq 1} \frac{\tilde{c}_n}{n^s}$$

により定める. $L(A, \iota, s)$ と $L(A, \iota \circ \tau, s)$ は, $\mathbf{Q}$ 上 τ に関して共役だから,

$$L_\alpha(s) = \frac{1}{2}(1 + \frac{\alpha^\sigma}{\sqrt{d}})L(A, \iota, s) + \frac{1}{2}(1 - \frac{\alpha^\sigma}{\sqrt{d}})L(A, \iota \circ \tau, s)$$

が成立する.

L- 関数 $L_\alpha(s)$ に付随する形式群を,

$$\hat{L}_\alpha(x_1,x_2) := g_\alpha^{-1}(g_\alpha(x_1)+g_\alpha(x_2)), \qquad g_\alpha(x) := \sum_{n\geq 1}\frac{\tilde{c}_n}{n}x^n$$

により定義する. この $\hat{L}_\alpha(s)$ に対して, 本田の定理は以下のように拡張される.

Theorem 4.1 $\hat{L}_\alpha(x_1,x_2)$ は $\mathcal{O}_k$ 上定義された形式群で, かつ, $\hat{L}_\alpha(x_1,x_2)$ は $\mathcal{O}$ 上で $\hat{E}(x_1,x_2)$ と強同型である. 但し, $\mathcal{O} := (\cap_{\mathfrak{p}/D_k}\mathcal{O}_{k,\mathfrak{p}})\cap k$.

Corollary 4.2 D_k を割らない任意の素数 p に対し, $\mathcal{O}_k$ における合同式 $\tilde{c}_p \equiv b_p \ mod\, p$ が成立する.

c_p の絶対値についても, Weil の評価式 : $|c_p| \leq 2\sqrt{p}$ が知られている. Corollary 4.2 と $\tilde{c}_p$ の定義式により, b_p がわかれば, $(D_k/p) = \pm 1$ に応じて, 整数 c_p, または, 整数 $c_p/\sqrt{d}$ が p を法として決まる. それ故, 少なくとも $p \geq 17$ に対しては, $b_p \bmod p$ から c_p が求まる. $p \leq 13$ についても, Theorem 4.1 から得られる別の合同式を用いれば, $b_p, b_{p^2}, \cdots$ 達から, c_p が求まる. このように, 具体的に $\hat{E}$ を与えれば, b_n 達から, $L_\alpha(s)$ の Dirichlet 係数を決定することができる. 同時に, $L(A,\iota,s)$ の Dirichlet 係数も決定される.

最後に, 数値例を与える.

Example 4.3 k を虚2次体 $\boldsymbol{Q}(\sqrt{-3})$ とし, $\zeta := (1+\sqrt{-3})/2$ とおく. E を *Weierstrass* モデル

$$E : Y^2 + (1-\zeta)XY - (1+\zeta)Y = X^3 + \zeta X^2 + (19+\zeta)X + 18 - 30\zeta$$
$$\Delta = -\zeta^2\cdot 3^3\cdot 7^2\cdot(3-\zeta)^4$$

で定義された k 上の楕円曲線とする. E は, $\Gamma_0(63)$ に対する *modular curve* である *(cf. [4])*. この場合, $d=3, \alpha = 2-\zeta$ に対し, 条件 $(Ei)-(Eiv)$ を満たす同種写像 $\varphi : E \to E^\sigma$ が存在する.

この時, $b_p, b_p\ mod\, p, c_p$ は, それぞれ, 以下のようになる. 尚, c_p は, E に対応する $\Gamma_0(63)$ の *new form* の *Fourier* 展開を計算することにより求めた.

p	$(-3/p)$	b_p	$b_p\ mod\, p$	c_p
2	-1	$-1+\zeta$	$1+\zeta$	$-\sqrt{3}$
3	0	0	0	0
5	-1	$27+7\zeta$	$2+2\zeta$	$2\sqrt{3}$
7	1	$57-196\zeta$	1	1
11	-1	$9403-26149\zeta$	$-2-2\zeta$	$-2\sqrt{3}$
13	1	$-234583+113464\zeta$	2	2
17	-1	$-34917577+7749873\zeta$	$-2-2\zeta$	$-2\sqrt{3}$
19	1	$95051239+3653700\zeta$	-4	-4
23	-1	$1705031103+24795239311\zeta$	$2+2\zeta$	$2\sqrt{3}$
29	-1	$21826646904619-28272514599109\zeta$	0	0

表により *Corollary 4.2* が $p \leq 29$ で確認できる. 逆に, *Corollary 4.2* と *Weil* の評価式を用いれば, c_p $(5 \leq p \leq 29)$ が表の $b_p \bmod p$ から求められる.

参考文献

[1] M. Atkin and H. Swinnerton-Dyer, *Modular forms on non congruence subgroups,* Proc. Symp. Pure Math XIX. Amer. Math. Soc., Providence 1971.

[2] C. Deninger and E. Nart, *Formal groups and L-series,* Comment. Math. Helv. 65 (1990), 318-333.

[3] A. Fröhlich, *Formal groups,* Lecture note in Mathematics, Springer, 1968.

[4] Y. Hasegawa, ***Q**-curves over quadratic fields,* Manuscripta Math. 94 (1997), 347-364.

[5] M. Hazewinkel, *Formal Groups and Applications,* New York, Academic Press 1978.

[6] T. Honda, *Formal groups and zeta-functions,* Osaka J. Math. 5 (1968), 199-213.

[7] T. Honda, *On the theory of commutative formal groups,* J. Math. Soc. Japan 22 (1970), 213-246.

[8] T. Honda, *Invariant Differentials and L-functions -Reciplocity law for quadratic fields and elliptic curves over* $\boldsymbol{Q}$, Rend. Sem. Mat. Univ. Padova, 49 (1973), 323-335.

[9] J. S. Milne, *On the Arithmetic of Abelian Varieties,* Invention Math. 17 (1972). 177-190.

[10] J. H. Silverman, *The Arithmetic of Elliptic curves,* Springer G.T.M. 106.

[11] J. Tate, *The Arithmetic of elliptic curves,* Invent. Math. 23 (1974),179-206.

[12] M. J. Vélu, *Isogénes entre courbes elliptiques,* C. R. Acad. Sc. Paris, t. 273 (1971), 238-241.

[13] A. Weil, *The field of definition of a variety,* Amer. J. Math.

Department of Mathematics,
Graduate School of Science,
Osaka University,
Toyonaka, Osaka 560-0043, Japan.
e-mail address : sairaiji @ mathsun01.math.sci.osaka-u.ac.jp